# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/003536

International filing date: 02 March 2005 (02.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-058444
Filing date: 03 March 2004 (03.03.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

P01-05039WO

PCT/JP2005/003536

# 日本国特許庁 08.3.2005
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

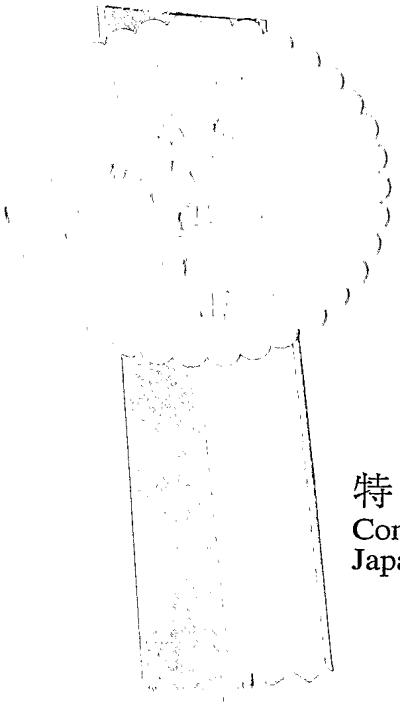
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　３月　３日

出願番号
Application Number: 特願２００４－０５８４４４

[ST. 10/C]: ［ＪＰ２００４－０５８４４４］

出願人
Applicant(s): パイオニア株式会社
株式会社テック・エキスパーツ
パイオニアシステムテクノロジー株式会社



２００５年　２月２２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０１３４３２

【書類名】　特許願
【整理番号】　58P0548
【あて先】　特許庁長官　殿
【国際特許分類】　G06K 17/00
【発明者】
　【住所又は居所】　埼玉県川越市山田字西町２５番地１　パイオニア株式会社　川越工場内
　【氏名】　野中　慶也
【発明者】
　【住所又は居所】　東京都大田区大森西４丁目１５番５号　株式会社テック・エキスパーツ内
　【氏名】　関根　能男
【発明者】
　【住所又は居所】　埼玉県川越市山田字西町２５番地１　パイオニア株式会社　川越工場内
　【氏名】　垂井　伸夫
【発明者】
　【住所又は居所】　埼玉県川越市山田字西町２５番地１　パイオニア株式会社　川越工場内
　【氏名】　新居　紀孝
【発明者】
　【住所又は居所】　東京都大田区大森西４丁目１５番５号　株式会社テック・エキスパーツ内
　【氏名】　杉野　竜二
【発明者】
　【住所又は居所】　東京都大田区大森西４丁目１５番５号　株式会社テック・エキスパーツ内
　【氏名】　青山　将士
【発明者】
　【住所又は居所】　埼玉県川越市山田字西町２５番地１　パイオニアシステムテクノロジー株式会社　埼玉事業所内
　【氏名】　岩路　博文
【発明者】
　【住所又は居所】　埼玉県川越市山田字西町２５番地１　パイオニアシステムテクノロジー株式会社　埼玉事業所内
　【氏名】　武藤　健
【特許出願人】
　【識別番号】　000005016
　【氏名又は名称】　パイオニア株式会社
【特許出願人】
　【識別番号】　502196463
　【氏名又は名称】　株式会社テック・エキスパーツ
【特許出願人】
　【識別番号】　500403929
　【氏名又は名称】　パイオニアシステムテクノロジー株式会社
【代理人】
　【識別番号】　100083839
　【弁理士】
　【氏名又は名称】　石川　泰男
　【電話番号】　03-5443-8461

【手数料の表示】
　【予納台帳番号】　007191
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9102133
　【包括委任状番号】　0213290

【書類名】特許請求の範囲
【請求項１】
携帯型の記録媒体を装着する装着手段と、当該電子機器固有の暗号化鍵を用いて所定の情報を暗号化し、暗号化情報として前記記録媒体に書き込む暗号化情報書込手段と、を備える電子機器であって、
前記記録媒体が前記装着手段に装着された場合に、当該記録媒体に記録されている暗号化情報を読み出す暗号化情報読出手段と、
前記暗号化鍵を用いて前記暗号化情報の解読を実行する解読実行手段と、
前記解読実行手段により前記暗号化情報が解読された場合には、当該電子機器を使用可能状態にさせる制御手段と、を備えることを特徴とする電子機器。
【請求項２】
請求項１に記載の電子機器において、
情報を保持する揮発性のメモリを更に備え、
前記装着手段に前記記録媒体が装着されていない状態で当該電子機器に電力が供給された場合に、前記メモリが情報保持状態にあるか否かを判別し、情報保持状態にない場合には、ユーザに対し前記記録媒体の装着を促す装着要求手段を更に備えることを特徴とする電子機器。
【請求項３】
請求項１又は２に記載の電子機器において、
前記制御手段は、前記暗号化情報が解読されて得られた情報と、予め設定された情報とが一致するか否かを判別し、一致する場合には、当該電子機器を使用可能状態にさせることを特徴とする電子機器。
【請求項４】
請求項１乃至３の何れかに記載の電子機器において、
前記解読実行手段により前記暗号化情報が解読されない場合には、警報出力を行う警報手段を更に備えることを特徴とする電子機器。
【請求項５】
携帯型の記録媒体を装着する装着手段と、当該電子機器固有の暗号化鍵を用いて所定の情報を暗号化し、暗号化情報として前記記録媒体に書き込む暗号化情報書込手段と、を備える電子機器における制御方法であって、
前記記録媒体が前記装着手段に装着された場合に、当該記録媒体に記録されている暗号化情報を読み出す工程と、
前記暗号化鍵を用いて前記暗号化情報の解読を実行する工程と、
前記解読実行手段により前記暗号化情報が解読された場合には、当該電子機器を使用可能状態にさせる工程と、を備えることを特徴とする電子機器における制御方法。
【請求項６】
携帯型の記録媒体を装着する装着手段と、当該電子機器固有の暗号化鍵を用いて所定の情報を暗号化し、暗号化情報として前記記録媒体に書き込む暗号化情報書込手段と、を備える電子機器に含まれるコンピュータを、
前記記録媒体が前記装着手段に装着された場合に、当該記録媒体に記録されている暗号化情報を読み出し、
前記暗号化鍵を用いて前記暗号化情報の解読を実行し、
前記解読実行手段により前記暗号化情報が解読された場合には、当該電子機器を使用可能状態にさせるように機能させることを特徴とするセキュリティプログラム。
【請求項７】
請求項６に記載のセキュリティプログラムがコンピュータ読み取り可能に記録されたことを特徴とする記録媒体。

【書類名】明細書
【発明の名称】電子機器及びその制御方法、並びにセキュリティプログラム等
【技術分野】
【０００１】
本発明は、電子機器の盗難防止又は抑止が可能な装置又は方法等の技術分野に関する。
【背景技術】
【０００２】
従来より、車載に搭載されるオーディオ装置やナビゲーション装置等の電子機器においては、盗難防止のための様々な盗難防止機構が備えられている。例えば、いわゆるクイックリリースという盗難防止機構においては、ユーザが車両から降りる際に当該装置自体を簡単に取り外し持ち出すことが可能になっており、また、いわゆるデタッチという盗難防止機構においては、ユーザが車両から降りる際に当該装置のパネル（例えば、操作・表示パネル）を簡単に取り外し持ち出すことが可能になっている。特許文献１には、このような盗難防止機構として、操作パネル等　を取り外し可能な技術が開示されている。
【０００３】
その他にも、例えば、ユーザが例えば操作・表示パネルを操作してパスワードを当該装置に入力することで、当該装置が起動するという盗難防止機構も存在する。
【特許文献１】特開２００３－２３７４８５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、例えば、クイックリリースやデタッチ等の従来の盗難防止機構においては、持ち出すもの自体の大きさが大きくユーザにとっては非常に不便であり、また、取り外し及び取り付けの作業が非常に煩わしいという不便さもあった。
【０００５】
また、パスワードを当該装置に入力する盗難防止機構においては、ユーザが例えば車両に乗り込む度に、パスワードを入力しなければならないという不便さがあり、更に、万一、ユーザがパスワードを忘れた場合には、当該装置が起動せず不便であった。
【０００６】
そこで、このような不便さの解消を一つの課題とし、より効果的に、電子機器の盗難を防止又は抑止することが可能な電子機器及びその制御方法、並びにセキュリティプログラム等を提供することを目的する。
【課題を解決するための手段】
【０００７】
上記課題を解決するため、請求項１に記載の発明は、携帯型の記録媒体を装着する装着手段と、当該電子機器固有の暗号化鍵を用いて所定の情報を暗号化し、暗号化情報として前記記録媒体に書き込む暗号化情報書込手段と、を備える電子機器であって、前記記録媒体が前記装着手段に装着された場合に、当該記録媒体に記録されている暗号化情報を読み出す暗号化情報読出手段と、前記暗号化鍵を用いて前記暗号化情報の解読を実行する解読実行手段と、前記解読実行手段により前記暗号化情報が解読された場合には、当該電子機器を使用可能状態にさせる制御手段と、を備えることを特徴とする。
【０００８】
請求項５に記載の発明は、携帯型の記録媒体を装着する装着手段と、当該電子機器固有の暗号化鍵を用いて所定の情報を暗号化し、暗号化情報として前記記録媒体に書き込む暗号化情報書込手段と、を備える電子機器における制御方法であって、前記記録媒体が前記装着手段に装着された場合に、当該記録媒体に記録されている暗号化情報を読み出す工程と、前記暗号化鍵を用いて前記暗号化情報の解読を実行する工程と、前記解読実行手段により前記暗号化情報が解読された場合には、当該電子機器を使用可能状態にさせる工程と、を備えることを特徴とする。
【０００９】

請求項６に記載のセキュリティプログラムは、携帯型の記録媒体を装着する装着手段と、当該電子機器固有の暗号化鍵を用いて所定の情報を暗号化し、暗号化情報として前記記録媒体に書き込む暗号化情報書込手段と、を備える電子機器に含まれるコンピュータを、前記記録媒体が前記装着手段に装着された場合に、当該記録媒体に記録されている暗号化情報を読み出し、前記暗号化鍵を用いて前記暗号化情報の解読を実行し、前記解読実行手段により前記暗号化情報が解読された場合には、当該電子機器を使用可能状態にさせるように機能させることを特徴とする。

【００１０】

請求項７に記載の記録媒体は、請求項６に記載のセキュリティプログラムがコンピュータ読み取り可能に記録されたことを特徴とする。

【発明を実施するための最良の形態】

【００１１】

以下、本願の最良の実施形態を添付図面に基づいて説明する。なお、以下に説明する実施の形態は、車載用オーディオ装置に対して本願を適用した場合の実施形態である。

【００１２】

先ず、図１を参照して、本実施形態における車載用オーディオ装置の構成及び機能を説明する。図１は、本実施形態における車載用オーディオ装置の概要ブロック例を示す図である。

【００１３】

図１に示すように、車載用オーディオ装置１は、情報再生部１１、情報出力部１２、表示・操作部１３、装着手段としてのメモリカード装着部１４、暗号化情報書込手段、暗号化情報読出手段、及び解読実行手段としてのメモリカード制御部１５、不揮発性メモリ（例えば、ＥＥＰＲＯＭ）１６、及び、制御手段、装着要求手段、及び警報出力手段としてのシステム制御部１７を備えて構成されており、当該車載用オーディオ装置１は、バッテリ電源１８又はＡＣＣ電源スイッチＯＮによりＡＣＣ電源から電力が供給されるようになっている。

【００１４】

情報再生部１１は、図示しないが、例えばＣＤ（Compact Disc）等の光ディスクの装填機構、所定のクランプ位置に載置された光ディスクに光ビームを照射して記録情報（例えば、楽曲データ）を光学的に読み取り電気信号に光電変換し出力する光ピックアップ、当該光ピックアップから出力された電気信号からＲＦ（Radio Frequency）信号等を生成して出力するＲＦアンプ、当該ＲＦ信号に所定の復調処理及び誤り訂正処理等を行いデジタル信号に変換するＤＳＰ（Digital Signal Processor）、及び、スピンドルモータ及び光ピックアップをサーボ制御するサーボ回路等を備えており、システム制御部１７の制御の下、光ディスクに記録された記録情報をデジタル音声信号として再生し、情報出力部１２に出力するようになっている。なお、情報再生部１１としては、特にＣＤに記録された記録情報を再生するものに限定されるものではなく、ＭＤ（Mini Disc）、ＤＶＤ（Digital Versatile Disc）等に記録された記録情報を再生するものであってもよい。

【００１５】

情報出力部１２は、図示しないが、情報再生部１１により出力されたデジタル音声信号を入力し、これをアナログ音声信号に変換するＤＡＣ（Digital-to-Analog Converter）、当該アナログ音声信号を増幅して出力するＡＭＰ（Amplifier）、及び増幅されたアナログ音声信号を音波として出力するスピーカ等を備えている。

【００１６】

表示・操作部１３は、ユーザからの各種指示（例えば、楽曲の再生や各種情報の表示等の指示）を受け付けるための複数の操作ボタンを備えており、ユーザにより操作ボタンが押下された場合に、その操作ボタンに応じた指示信号をシステム制御部１７に出力するようになっている。また、表示・操作部１３は、液晶パネル等の表示パネルを有し、システム制御部１７の制御の下、各種情報や選択メニュー等を表示する。

【００１７】

また、詳しくは後述するが、表示・操作部１３は、ユーザからの鍵管理メニュー表示指示に基づき、システム制御部１７の制御の下、鍵管理メニューを表示パネル上に表示するようになっており、ユーザは、当該鍵管理メニューにおいて、操作ボタンを操作し、暗号化鍵の発行／回収、暗号化鍵によるセキュリティＯＮ／ＯＦＦ設定、暗号化鍵の有効／無効設定等を行うことができる。

【００１８】

メモリカード装着部１４には、携帯型の記録媒体の一例としてのメモリカード（本実施形態においては、公知のマジックゲートメモリスティック（登録商標）を適用）２０が挿入され、装着される。また、メモリカード装着部１４は、メモリカード２０の装着状態を電気的又は機械的に検出する検出部を有しており、メモリカード２０が装着されたことを検出すると、その検出信号をメモリカード制御部１５及びシステム制御部１７に出力するようになっている。

【００１９】

メモリカード２０には、図示しないが、例えばＬＳＩ（Large Scale Integrated circuit）から構成された暗号化演算回路、及び情報を記録するためのフラッシュメモリを備えており、更に、当該カード固有（カード毎に異なる）の媒体識別情報（ＩＤ）や暗号化鍵を記憶保持するための不揮発性メモリを備えている。この媒体識別情報は、当該メモリカード２０の製造時又は出荷時に当該メモリカード２０に割り当てられ不揮発性メモリに記憶される。

【００２０】

メモリカード制御部１５もまた、図示しないが、例えばＬＳＩ（Large Scale Integrated circuit）から構成された暗号化演算回路を備えている。また、不揮発性メモリ１６には、当該車載用オーディオ装置１の当該装置固有（装置毎に異なる）の機器識別情報（ＩＤ）を記憶保持されており、この機器識別情報は、例えば、当該車載用オーディオ装置１の製造時又は出荷時に当該装置１に割り当てられ、不揮発性メモリ１６に記憶される。

【００２１】

そして、メモリカード２０がメモリカード装着部１４に装着された場合に（メモリカード装着部１５からの検出信号があった場合に）、メモリカード制御部１５とメモリカード２０との間でお互いの識別情報（機器識別情報（ＩＤ）と媒体識別情報（ＩＤ））をメモリカード制御部１５とメモリカード２０間の通信経路を介して交換し合い、正当な（著作権保護に対応している）装置又は媒体であるか否かを認証し合う（相互認証）ようになっている。

【００２２】

また、上記認証結果が正常であった場合には、その後の情報のやり取りは暗号化された上で行なわれることになる。この暗号化に使用される鍵としては、メモリカード制御部１５の暗号化演算回路のみが使用する装置暗号化鍵と、メモリカード２０の暗号化演算回路のみが使用するカード暗号化鍵と、メモリカード制御部１５及びメモリカード２０の暗号化演算回路が使用する共通暗号化鍵の３つが存在する。そのうち、装置暗号化鍵は、当該車載用オーディオ装置１固有の暗号化鍵であり、例えば機器識別情報に基づいて生成され不揮発性メモリ１６に予め記憶保持される。また、カード暗号化鍵は、当該メモリカード２０固有の暗号化鍵であり、例えば媒体識別情報に基づいて生成されメモリカード２０の不揮発性メモリに予め記憶保持される。

【００２３】

また、共通暗号化鍵は、当該車載用オーディオ装置１及びメモリカード２０とに共通の暗号化鍵であり、上記相互認証毎に当該メモリカード制御部１５とメモリカード２０の双方で生成される。より具体的には、当該メモリカード制御部１５とメモリカード２０の暗号化演算回路は、上記相互認証において得られた機器識別情報と媒体識別情報とに基づいて共通の暗号化鍵を生成する。この共通暗号化鍵の生成には、公知の様々な手法を適用可能であるが、一つの例として、暗号化演算回路は、媒体識別情報である数桁の番号と機器識別情報である数桁の番号とを繋ぎ合わせ、その番号に基づき例えばハッシュ関数による

演算手法で共通暗号化鍵を生成する（与えられた番号から固定長の疑似乱数を生成し、それを共通暗号化鍵とする）。

【００２４】

このように生成された共通暗号化鍵は、当該車載用オーディオ装置１と当該メモリカード２０の組合せ固有の共通暗号化鍵となる。なお、当該共通暗号化鍵は、媒体識別情報のみに基づいて生成されるように構成してもよい。

【００２５】

ここで、これらの暗号化鍵が用いられて、メモリカード制御部１５とメモリカード２０との間で行なわれる情報のやり取り等について図２及び図３を参照して説明する。なお、図２は、メモリカード２０への暗号化情報の書き込み時におけるメモリカード制御部１５とメモリカード２０における情報処理及び情報やり取りを示すシーケンス図であり、図３は、メモリカード２０からの暗号化情報の読み出し時におけるメモリカード制御部１５とメモリカード２０における情報処理及び情報やり取りを示すシーケンス図である。

【００２６】

先ず、メモリカード２０への暗号化情報の書き込み時においては、図２に示すように、メモリカード制御部１５の暗号化演算回路は、例えばシステム制御部１７から指示された情報（例えば、パスワード）を装置暗号化鍵を用いて暗号化して暗号化情報を生成する（ステップＳ１０１）。続いて、メモリカード制御部１５の暗号化演算回路は、共通暗号化鍵を用いて装置暗号化鍵を暗号化して（ステップＳ１０２）、これをメモリカード２０の暗号化演算回路に渡す（ステップＳ１０３）。

【００２７】

これに応じて、メモリカード２０の暗号化演算回路は、共通暗号化鍵を用いて装置暗号化鍵を複合化した後、カード暗号化鍵を用いて装置暗号化鍵を暗号化して（ステップＳ１０４）、これをメモリカード制御部１５の暗号化演算回路に渡す（ステップＳ１０５）。

【００２８】

これに応じて、メモリカード制御部１５の暗号化演算回路は、上記暗号化した暗号化情報と、メモリカード２０の暗号化演算回路からの上記カード暗号化鍵により暗号化された装置暗号化鍵を、メモリカード２０におけるフラッシュメモリに書き込む（ステップＳ１０６）。

【００２９】

次に、メモリカード２０からの暗号化情報の読み出しにおいては、図３に示すように、メモリカード制御部１５の暗号化演算回路は、システム制御部１７からの指示の下、フラッシュメモリに書き込まれた暗号化情報と、カード暗号化鍵により暗号化された装置暗号化鍵を読み出す（ステップＳ２０１）。このとき、メモリカード制御部１５の暗号化演算回路は、暗号化情報が不正にコピーされたものであるか否かをチェックする。続いて、メモリカード制御部１５の暗号化演算回路は、カード暗号化鍵により暗号化された装置暗号化鍵をメモリカード２０の暗号化演算回路に渡す（ステップＳ２０２）。

【００３０】

これに応じて、メモリカード２０の暗号化演算回路は、カード暗号化鍵を用いて装置暗号化鍵を複合化した後、共通暗号化鍵を用いて装置暗号化鍵を暗号化して（ステップＳ２０３）、これをメモリカード制御部１５の暗号化演算回路に渡す（ステップＳ２０４）。

【００３１】

これに応じて、メモリカード制御部１５の暗号化演算回路は、共通暗号化鍵を用いて装置暗号化鍵を複合化した後、その装置暗号化鍵を用いて暗号化情報を複合化（解読）して、元の情報を得て、システム制御部１７に渡す（ステップＳ２０５）。

【００３２】

こうして、車載用オーディオ装置１とメモリカード２０とでセキュリティシステムを構成することになる。

【００３３】

システム制御部１７は、演算機能を有するＣＰＵ、揮発性のメモリとしてのＲＡＭ、及

び各種処理プログラム（プログラムを含む：このプログラムは、例えばインターネット上の所定のサーバからダウンロードされるようにしてもよいし、フレキシブルディスク（例えば、ＣＤ－ＲＯＭ等）の記録媒体に記録されて当該記録媒体のドライブを介して読み込まれるようにしてもよい。）やデータを記憶するＲＯＭ等を備えている。また、システム制御部１７におけるＲＡＭには、バッテリ電源１８から電力が供給されている間は、情報が保持される。

【００３４】

そして、ＣＰＵがＲＯＭに記憶されたプログラムを実行することにより、コンピュータとしてのシステム制御部１７は、車載用オーディオ装置１全体を統括制御し、表示・操作部１３における操作ボタンを介したユーザ指示に応じて、光ディスクから記録情報を再生したり、表示パネルに各種情報を表示する等の車載用オーディオ装置１における機能を実現するように制御を行うようになっている。

【００３５】

更に、メモリカード装着部１４にメモリカード２０が装着されていない状態で当該車載用オーディオ装置１に電力が供給されたとき、システム制御部１７は、ＲＡＭが情報保持状態にあるか否かを判別し、情報保持状態にない場合には、ユーザに対しメモリカード装着部１４にメモリカード２０の装着を促す。そして、メモリカード２０がメモリカード装着部１４に装着され、メモリカード制御部１５により暗号化情報が読み出され、復号化（解読）された情報がシステム制御部１７に入力された場合には、システム制御部１７は、上記暗号化情報が解読されて得られた情報と、予め設定された情報とが一致するか否かを判別し、一致する場合には、当該車載用オーディオ装置１を使用可能状態にさせるようになっている。

【００３６】

ここで、使用可能状態とは、車載用オーディオ装置１における機能が正常に起動して、当該機能を発揮し得る状態をいい、例えば、車載用オーディオ装置１が、ユーザからの操作ボタンを介した指示を受付け、情報再生部１１に装填された光ディスクからの記録情報の再生が可能となる状態である。これとは逆に、使用不可状態とは、車載用オーディオ装置１における機能が正常に起動せず、停止又は強制ロックされ、ユーザからの操作ボタンを介した指示を受け付けず、情報再生部１１に装填された光ディスクからの記録情報の再生も不可となる状態である。

【００３７】

なお、システム制御部１７は、メモリカード制御部１５により暗号化情報が解読された場合に、その情報を受け、当該車載用オーディオ装置１を使用可能状態にさせるように構成してもよい。

【００３８】

また、システム制御部１７は、鍵管理メニューを表示・操作部１３における表示パネルに表示させ、ユーザからの操作ボタンを介した指示に基づき、上記暗号化鍵の発行／回収、暗号化鍵によるセキュリティＯＮ／ＯＦＦ設定、暗号化鍵の有効／無効設定等を行う。上記鍵管理メニューにて設定された内容は、不揮発性メモリ１６に記憶されることになる。

【００３９】

ここで、暗号化鍵の発行とは、例えば図２に示すステップＳ１０６のように、カード暗号化鍵により暗号化された装置暗号化鍵が暗号化情報と共にメモリカード２０におけるフラッシュメモリに書き込まれることをいい、暗号化鍵の回収とは、メモリカード２０におけるフラッシュメモリに書き込まれた当該暗号化された装置暗号化鍵及び暗号化情報が消去されることをいうものとする。また、暗号化鍵の無効設定とは、メモリカード２０におけるフラッシュメモリに書き込まれた当該暗号化された装置暗号化鍵を使用不可とする設定をいうものとする。

【００４０】

次に、図４乃至図６を参照して、本実施形態における車載用オーディオ装置１の動作を

説明する。

【００４１】

図４は、システム制御部１７におけるメインルーチンの一例を示すフローチャートであり、図５は、図４に示すステップＳ１３の鍵管理処理の詳細を示すフローチャートである。また、図６（Ａ）は、図５に示すステップＳ２３の暗号化鍵発行処理を示すフローチャートであり、図６（Ｂ）は、図５に示すステップＳ２５の暗号化鍵回収処理を示すフローチャートであり、図６（Ｃ）は、図５に示すステップＳ２７のセキュリティＯＮ／ＯＦＦ設定処理を示すフローチャートであり、図６（Ｄ）は、図５に示すステップＳ２９の暗号化鍵有効／無効設定処理を示すフローチャートである。

【００４２】

先ず、例えば車載用オーディオ装置１の電源が投入され、バッテリ電源１８からの電力が供給されることにより当該オーディオ装置１が動作した初期の段階では、装置使用不可状態となっており、図４に示す処理において、システム制御部１７により例えば不揮発性メモリ１６が参照され、セキュリティＯＮ設定であるか否か、つまり、暗号化鍵によるセキュリティの実行がなされているか否かが判別され（ステップＳ１）、セキュリティＯＮ設定である場合には（ステップＳ１：Ｙ）、ステップＳ２に移行し、セキュリティＯＮ設定でない（セキュリティＯＦＦ設定である）場合には（ステップＳ２：Ｎ）、ステップＳ９に移行する。

【００４３】

ステップＳ２では、揮発性メモリであるＲＡＭが情報保持状態にある（メモリ保持モードから起動したか）か否かが判別され、情報保持状態にない（例えば、当該装置１が外されることによりバッテリ電源１８からの電力供給が切断（バックアップ電源断）しＲＡＭの情報が消去されている）場合には（ステップＳ２：Ｎ）、ステップＳ３に移行し、情報保持状態にある場合には（ステップＳ２：Ｙ）、ステップＳ９に移行する。

【００４４】

ステップＳ３では、メモリカード装着部１５にメモリカード２０が装着されているか否かが判別され、メモリカード２０が装着されていない場合には（ステップＳ３：Ｎ）、ステップＳ４に移行され、メモリカード２０が装着されている（メモリカード装着部１５からの検出信号がある）場合には（ステップＳ３：Ｙ）、ステップＳ５に移行する。

【００４５】

ステップＳ４では、メモリカード２０の装着を促すメッセージ、例えば、「メモリカードを装着してください」等のメッセージが表示・操作部１３における表示パネル上に表示される。なお、システム制御部１７は、当該メッセージを情報出力部１２におけるスピーカから音声出力させてメモリカード２０の装着を促すように構成してもよい。

【００４６】

ステップＳ５では、メモリカード２０が正当な媒体であるか否かのメモリカードチェックが実行される。

【００４７】

ステップＳ５のメモリカードチェックにおいては、例えばシステム制御部１７がメモリカード制御部１５に対してメモリカードチェック指令を与えることにより、上述したように、メモリカード制御部１５とメモリカード２０との間でお互いの識別情報（機器識別情報と媒体識別情報）が通信経路を介して交換し合われ、上述した相互認証が行なわれる。

【００４８】

そして、当該認証結果が良好である場合には、メモリカード制御部１５とメモリカード２０の暗号化演算回路により上記相互認証において得られた機器識別情報と媒体識別情報とに基づいて共通暗号化鍵が夫々生成される。

【００４９】

続いて、メモリカード制御部１５は、メモリカード２０に暗号化情報及び暗号化された装置暗号化鍵が書き込まれているか否かを確認し、書き込まれている場合には、上述した図３に示すステップＳ２０１からＳ２０５までの情報処理及び情報やり取りが行なわれる

。

【００５０】

そして、システム制御部１７によりメモリカード制御部１５からの復号化された情報と、予めユーザ等により設定され、例えば不揮発性メモリ１６に記憶された情報（例えば、パスワード）、とが一致するか否かが判別され、一致する場合には、メモリカードチェックが良好となり（ステップＳ５：ＯＫ）、ステップＳ９に移行する。

【００５１】

一方、メモリカードチェックおいて上記認証結果が良好でない、例えば著作権保護に対応していない普通のメモリカードである場合には、メモリカードチェックが良好でないと判別され（ステップＳ５：ＮＧ）、その旨のメッセージが表示・操作部１３における表示パネル上に表示される（ステップＳ６）。また、例えば、暗号化情報がメモリカード２０に書き込まれていない場合、当該暗号化鍵が無効設定になっている場合、又は当該暗号化鍵により暗号化情報の解読ができない（暗号化鍵が不正である）場合には、メモリカードチェックが良好でないと判別され、その旨のメッセージが表示・操作部１３における表示パネル上に表示される。そして、メモリカードチェックが良好でない回数が、予め規定された規定回数でない（規定回数に達していない）場合には（ステップＳ７：Ｎ）、ステップＳ５に戻り、メモリカードチェックが再び行われる。

【００５２】

また、メモリカードチェックが良好でない回数が、予め規定された規定回数である（規定回数に達した）場合には（ステップＳ７：Ｙ）、車載用オーディオ装置１の使用不可状態が継続され（ステップＳ８）、例えば、情報再生部１１におけるスピーカから警報（例えば、大音量のサイレンや盗難された装置である旨のメッセージ等）が出力される。また、車載用オーディオ装置１へのバッテリ電源１８からの電力供給が切断するように構成してもよい。

【００５３】

ステップＳ９では、システム制御部１７によって車載用オーディオ装置１の装置使用可能状態に切り換えられ、車載用オーディオ装置１における機能が正常に起動される。これにより、システム制御部１７は、ユーザからの表示・操作部１３における操作ボタンを介した情報再生指示を受け付けると（ステップＳ１０：Ｙ）、情報再生部１１を制御して光ディスクから記録情報を再生させる（ステップＳ１１）ようになる。また、この他にも、ユーザからの表示・操作部１３における操作ボタンを介した指示に応じて、パネル表示等の所定の機能を実行するようになるが図示を省略している。

【００５４】

そして、システム制御部１７がユーザからの表示・操作部１３における操作ボタンを介した鍵管理メニュー表示指示を受け付けると（ステップＳ１２：Ｙ）、図５に示す鍵管理処理に移行する（ステップＳ１３）。

【００５５】

図５に示す鍵管理処理においては、先ず、表示・操作部１３における表示パネル上に鍵管理メニューが表示される（ステップＳ２１）。この鍵管理メニュー上には、「暗号化鍵の発行」、「暗号化鍵の回収」、「セキュリティＯＮ／ＯＦＦ設定」、「暗号化鍵の有効／無効設定」、及び「鍵管理メニュー終了」の選択項目が表示されている。

【００５６】

そして、システム制御部１７がユーザからの表示・操作部１３における操作ボタンを介した「暗号化鍵の発行」の選択指示を受け付けると（ステップＳ２２：Ｙ）、図６（Ａ）に示す暗号化鍵発行処理に移行する（ステップＳ２３）。

【００５７】

一方、システム制御部１７がユーザからの表示・操作部１３における操作ボタンを介した「暗号化鍵の回収」の選択指示を受け付けると（ステップＳ２４：Ｙ）、図６（Ｂ）に示す暗号化鍵回収処理に移行する（ステップＳ２５）。

【００５８】

一方、システム制御部１７がユーザからの表示・操作部１３における操作ボタンを介した「セキュリティＯＮ／ＯＦＦ設定」の選択指示を受け付けると（ステップＳ２６：Ｙ）、図６（Ｂ）に示すセキュリティＯＮ／ＯＦＦ設定処理に移行する（ステップＳ２７）。

【００５９】

一方、システム制御部１７がユーザからの表示・操作部１３における操作ボタンを介した「暗号化鍵の有効／無効設定」の選択指示を受け付けると（ステップＳ２８：Ｙ）、図６（Ｂ）に示す暗号化鍵の有効／無効設定処理に移行する（ステップＳ２９）。

【００６０】

一方、システム制御部１７がユーザからの表示・操作部１３における操作ボタンを介した「鍵管理メニュー終了」の選択指示を受け付けると（ステップＳ３０：Ｙ）、図４に示す処理に戻る。

【００６１】

次に、図６（Ａ）に示す暗号化鍵発行処理について説明する。

【００６２】

図６（Ａ）に示す暗号化鍵発行処理においては、システム制御部１７により例えば不揮発性メモリ１４が参照されて、暗号化鍵の残り本数（暗号化鍵の発行可能な最大本数（例えば、４本）から暗号化鍵の現時点における発行本数（例えば、２本）を引いた本数）が「０」であるか否かが判別される（ステップＳ５１）。

【００６３】

ここで、暗号化鍵の発行可能な最大本数によって、当該オーディオ装置１により発行可能な暗号化鍵の本数が制限されており、セキュリティの強化を図ると共に、例えば家族による使用や、紛失等に備えて複数発行（言い換えれば、複数のメモリカードに、上記暗号化された装置暗号化鍵及び上記暗号化情報を書き込む）できるようになっている。この暗号化鍵の発行可能な最大本数は、例えば、ユーザにより表示・操作部１３における操作ボタンを介して任意に設定されるように構成してもよいし、メーカ側にて予め設定されるようにように構成してもよい。

【００６４】

そして、暗号化鍵の残り本数が「０」である場合には（ステップＳ５１：＝０）、これ以上暗号化鍵を発行することができないので、その旨のメッセージが表示パネル上に表示された後、当該暗号化鍵発行処理が終了し、図５に示す処理に戻る。一方、暗号化鍵の残り本数が「０」でない場合には（ステップＳ５１：０でない）、メモリカードチェックが実行される（ステップＳ５２）。なお。メモリカード２０がメモリカード装着部１４に装着されていない場合には、メモリカード２０の装着を促すメッセージが表示・操作部１３における表示パネル上に表示され、ユーザによりメモリカード２０の装着がなされた場合に、当該メモリカードチェックが実行されることになる。

【００６５】

ステップＳ５２のメモリカードチェックにおいては、システム制御部１７がメモリカード制御部１５に対してメモリカードチェック指令を与えることにより、上述したように、メモリカード制御部１５とメモリカード２０との間でお互いの識別情報（機器識別情報と媒体識別情報）を通信経路を介して交換し合い、上述した相互認証が行われ、当該認証結果が良好である場合には、メモリカードチェックが良好となり（ステップＳ５２：ＯＫ）、ステップＳ５３に移行する。なお、当該認証結果が良好である場合には、メモリカード制御部１５とメモリカード２０の暗号化演算回路により上記相互認証において得られた機器識別情報と媒体識別情報とに基づいて共通暗号化鍵が夫々生成される。

【００６６】

一方、上記認証結果が良好でない、例えば著作権保護に対応していない普通のメモリカードである場合には、メモリカードチェックが良好でないと判別され（ステップＳ５２：ＮＧ）、その旨のメッセージが表示パネル上に表示された後、当該暗号化鍵発行処理が終了し、図５に示す処理に戻る。

【００６７】

ステップＳ５３では、システム制御部１７がメモリカード制御部１５に対して、予め設定された情報（例えば、ユーザが、表示・操作部１３における操作ボタンを操作することによって入力されたパスワード）を指示すると共に暗号化鍵の発行指令を与える。これにより、上述した図２に示すステップＳ１０１からＳ１０６までの情報処理及び情報やり取りが行なわれ、カード暗号化鍵により暗号化された装置暗号化鍵が暗号化情報と共にメモリカード２０におけるフラッシュメモリに書き込まれる。

【００６８】

こうして、車載用オーディオ装置１のセキュリティ用の新たなメモリカード２０が発行、言い換えれば、かかるメモリカード２０自体が鍵となって生成されることになる。このように発行されるメモリカード２０の鍵の最大数は、暗号化鍵の発行可能な最大本数と同じである。

【００６９】

次いで、不揮発性メモリ１４に記憶されている暗号化鍵の残り本数が１本減らされ（ステップＳ５４）、セキュリティＯＮ設定がなされる（ステップＳ５５）。また、メモリカード２０に書き込まれた上記暗号化鍵を示す情報（例えば、当該暗号化鍵に対応付けられた識別情報）が機器識別情報及び媒体識別情報に対応付けられて例えば不揮発性メモリ１４に記憶された暗号化鍵リストに登録される。

【００７０】

次に、図６（Ｂ）に示す暗号化鍵回収処理について説明する。

【００７１】

図６（Ｂ）に示す暗号化鍵回収処理においては、システム制御部１７により例えば不揮発性メモリ１４が参照されて、暗号化鍵の残り本数が「最大」であるか否かが判別される（ステップＳ６１）。暗号化鍵の残り本数が「最大」である場合には（ステップＳ６１：＝ＭＡＸ）、暗号化鍵が全く発行されていないので、その旨のメッセージが表示パネル上に表示された後、当該暗号化鍵回収処理が終了し、図５に示す処理に戻る。一方、暗号化鍵の残り本数が「最大」でない場合には（ステップＳ６１：ＭＡＸでない）、メモリカードチェックが実行される（ステップＳ６２）。なお、かかるメモリカードチェックは、上述したステップＳ５２におけるメモリカードチェックと同様であるので説明を省略する。そして、相互認証が良好である場合には、システム制御部１７は、例えば不揮発性メモリ１６に記憶された暗号化鍵リストを参照して、機器識別情報及び媒体識別情報に対応する暗号化鍵を示す情報が登録されているか否かを判別し、登録されている場合には、メモリカード制御部１５に対して暗号化鍵の回収指令を与える。これにより、メモリカード制御部１５がメモリカード２０のフラッシュメモリに書き込まれている上記装置暗号化鍵及び暗号化情報を消去する。

【００７２】

次いで、不揮発性メモリ１４に記憶されている暗号化鍵の残り本数が１本増やされる（ステップＳ６４）と共に、例えば不揮発性メモリ１６に記憶された暗号化鍵リストに登録されている当該機器識別情報及び媒体識別情報に対応する暗号化鍵を示す情報が消去される。

【００７３】

次いで、暗号化鍵の残り本数が「最大」であるか否かが判別され（ステップＳ６５）、暗号化鍵の残り本数が「最大」である場合には（ステップＳ６５：＝ＭＡＸ）、セキュリティＯＦＦ設定がなされ（ステップＳ６６）、当該暗号化鍵発行処理が終了し、図５に示す処理に戻る。一方、暗号化鍵の残り本数が「最大」でない場合には（ステップＳ６５：＝ＭＡＸでない）、そのまま、当該暗号化鍵発行処理が終了し、図５に示す処理に戻る。

【００７４】

次に、図６（Ｃ）に示すセキュリティＯＮ／ＯＦＦ設定処理について説明する。

【００７５】

図６（Ｃ）に示すセキュリティＯＮ／ＯＦＦ設定処理においては、システム制御部１７により例えば不揮発性メモリ１４が参照されて、暗号化鍵の残り本数が「最大」であるか

否かが判別される（ステップＳ７１）。暗号化鍵の残り本数が「最大」である場合には（ステップＳ７１：＝ＭＡＸ）、暗号化鍵が全く発行されていないので、その旨のメッセージが表示パネル上に表示された後、当該セキュリティＯＮ／ＯＦＦ設定処理が終了し、図５に示す処理に戻る。

【００７６】

一方、暗号化鍵の残り本数が「最大」でない場合には（ステップＳ７１：ＭＡＸでない）、メモリカードチェックが実行される（ステップＳ７２）。なお、かかるメモリカードチェックは、上述したステップＳ５２におけるメモリカードチェックに加えて、更に、メモリカード制御部１５がメモリカード２０に書き込まれている上記装置暗号化鍵が正しい鍵であるか否かもチェックされる。

【００７７】

例えば、ここでの相互認証が良好である場合に、メモリカード制御部１５の暗号化演算回路は、メモリカード２０に書き込まれた暗号化された装置暗号化鍵を読み出し、これをメモリカード２０の暗号化演算回路に渡す。これに応じて、メモリカード２０の暗号化演算回路は、カード暗号化鍵を用いて装置暗号化鍵を複合化した後、共通暗号化鍵を用いて装置暗号化鍵を暗号化して、これをメモリカード制御部１５の暗号化演算回路に渡す。これに応じて、メモリカード制御部１５の暗号化演算回路は、共通暗号化鍵を用いて装置暗号化鍵を複合化し、当該装置暗号化鍵が車載用オーディオ装置１の装置暗号化鍵であるか否かを判別し、その判別結果をシステム制御部１７に伝える。

【００７８】

そして、当該装置暗号化鍵が車載用オーディオ装置１の装置暗号化鍵でない場合には、メモリカードチェックが良好でないと判別され（ステップＳ７２：ＮＧ）、当該暗号化鍵が不正であるのでセキュリティ設定を変更できない旨のメッセージが表示パネル上に表示され（ステップＳ７３）た後、当該セキュリティＯＮ／ＯＦＦ設定処理が終了し、図５に示す処理に戻る。

【００７９】

一方、当該装置暗号化鍵が車載用オーディオ装置１の装置暗号化鍵である場合には、メモリカードチェックが良好であると判別され（ステップＳ７２：ＯＫ）、続いて、現在のセキュリティ設定状態が判別され（ステップＳ７４）、セキュリティＯＦＦ設定である場合には（ステップＳ７４：ＯＦＦ）、セキュリティＯＮ設定がなされ（ステップＳ７５）、セキュリティＯＮ設定である場合には（ステップＳ７４：ＯＮ）、セキュリティＯＮ設定がなされ（ステップＳ７６）、当該セキュリティＯＮ／ＯＦＦ設定処理が終了し、図５に示す処理に戻る。

【００８０】

次に、図６（Ｄ）に示す暗号化鍵有効無効設定処理について説明する。

【００８１】

図６（Ｄ）に示す暗号化鍵有効無効設定処理においては、システム制御部１７により不揮発性メモリ１６に記憶された暗号化鍵リストが読み出されて、表示パネル上に選択可能に表示される（ステップＳ８１）。この暗号化鍵リストには、図６（Ａ）に示す暗号化鍵発行処理にて発行された上記暗号化鍵を示す情報がリスト形式で表示される。

【００８２】

そして、ユーザが、表示・操作部１３における操作ボタンが暗号化鍵リストに表示された所望の暗号化鍵を示す情報を選択すると、選択された暗号化鍵を示す情報がシステム制御部１７により受け付けられ（ステップＳ８２）、その暗号化鍵が有効であるか否かが判別される（ステップＳ８３）。

【００８３】

当該暗号化鍵が有効である場合には（ステップＳ８３：Ｙ）、当該暗号化鍵の無効設定がなされ（ステップＳ８４）、続いて、有効な暗号化鍵があるか否かが判別され（ステップＳ８５）、ある場合には（ステップＳ８５：Ｙ）、当該暗号化鍵有効無効設定処理が終了し、図５に示す処理に戻る。一方、有効な暗号化鍵がない場合には（ステップＳ８５：

Ｎ）、セキュリティＯＦＦ設定がなされ（ステップＳ８６）、図５に示す処理に戻る。

【００８４】

一方、ステップＳ８３の処理において、当該暗号化鍵が有効でない（無効である）場合には（ステップＳ８３：Ｎ）、メモリカードチェックが実行される（ステップＳ８７）。なお、かかるメモリカードチェックは、上述したステップＳ７２におけるメモリカードチェックと同様であるので説明を省略する。

【００８５】

そして、メモリカードチェックが良好である場合には（ステップＳ８７：ＯＫ）、選択された暗号化鍵の有効設定がなされ（ステップＳ８８）、メモリカードチェックが良好でない場合には（ステップＳ８７：ＮＧ）、当該暗号化鍵が不正であるので有効設定できない旨のメッセージが表示パネル上に表示され（ステップＳ８９）た後、当該暗号化鍵有効無効設定処理が終了し、図５に示す処理に戻る。

【００８６】

以上説明したように上記実施形態によれば、セキュリティＯＮ設定がなされている場合に、例えば、当該車載用オーディオ装置１が盗難された場合であっても、当該車載用オーディオ装置１におけるメモリカード制御部１５によって発行された暗号鍵（カード暗号鍵により暗号化された装置暗号鍵）及び暗号化情報が書き込まれたメモリカード２０がなければ、当該車載用オーディオ装置１が正常に起動しないばかりか、スピーカから警報が発せられるので、より効果的に当該車載用オーディオ装置１の盗難を防止又は抑止することが可能となる。

【００８７】

また、メモリカード２０は、持ち運び便利な小型、軽量であるため、当該車載用オーディオ装置１を起動させる鍵として、より利便性が高いということができる。

【００８８】

また、例えば、メモリカード２０におけるフラッシュメモリに書き込まれた暗号鍵（カード暗号鍵により暗号化された装置暗号鍵）及び暗号化情報が、他のメモリカード２０に不正にファイルコピーされたとしても、メモリカード２０におけるカード暗号鍵は固有（他のメモリカード２０のカード暗号鍵とは異なる）ものであるため、装置暗号鍵の抽出はできず、従って、暗号化情報の解読を行うことができないため、当該車載用オーディオ装置１が正常に起動しない。

【００８９】

更にまた、ユーザがメモリカード制御部１５によって発行された暗号鍵及び暗号化情報が書き込まれたメモリカード２０自体を紛失又は発見（紛失後に見つかった）した場合に備えて、上記発行された上記暗号化鍵を無効又は有効に設定することができる。

【００９０】

なお、上記実施形態において、当該車載用オーディオ装置１に無線基地局と通信可能な通信器を備えさせ、当該車載用オーディオ装置１が、無線基地局、及び、移動体通信網やインターネット等を介してセキュリティセンター等のサーバに接続可能に構成し、図４に示すステップＳ７においてメモリカードチェックが良好でない回数が予め規定された規定回数である場合に、当該車載用オーディオ装置１からセキュリティセンター等のサーバに接続し、当該装置１が盗難された旨などの警報通知するように構成する。更に、当該車載用オーディオ装置１にＧＰＳ受信機を備えさせ、上記盗難された旨と共に当該装置１の位置情報（緯度及び経度）を通知するように構成してもよい。このように構成すれば、より一層、当該車載用オーディオ装置１の盗難を防止又は抑止することが可能となると共に、盗難された場合にも、その場所を把握することができる。

【００９１】

また、上記実施形態においては、セキュリティＯＮ設定であり、かつ情報保持状態にない場合に、メモリカード２０の装着がなければ、メモリカード２０の装着を促すように構成したが、別の例として、ＡＣＣ電源スイッチがＯＮされる（ＡＣＣ電源からの電力供給がなされる）毎に、メモリカード２０の装着がなければ、メモリカード２０の装着を促す

ように構成してもよい。

【００９２】

また、上記実施形態においては、メモリカード２０の一例としてマジックゲートメモリスティック（登録商標）を適用したが、これに限定されるものではなく、媒体毎に固有の媒体識別情報（ＩＤ）を持つ、例えばＳＤメモリカードや、セキュアＭＭＣなどの記録媒体であれば、適用可能である。

【００９３】

また、上記実施形態においては、電子機器の一例として車載用オーディオ装置１を適用したが、これに限定されるものではなく、例えば、車載用ＡＶ（Audio Visual）装置、車載用ナビゲーション装置、及び車載用ＡＶ・ナビゲーション装置、更には、車載用に限定されず、建物内に設置される家庭用、業務用等のオーディオ装置、ＡＶ装置等に対しても適用可能である。

【００９４】

また、上記実施形態において、メモリカード制御部１５における暗号化演算回路は、ハードウェア的に構成されても、ソフトウェア的に、つまり、所定のセキュリティプログラムがＣＰＵに実行されることにより構成されてもよい。また、メモリカード制御部１５における暗号化演算回路における機能をシステム制御部１７におけるＣＰＵが所定のセキュリティプログラムを実行することにより実現するように構成されてもよい（この場合、本願の暗号化情報書込手段、暗号化情報読出手段、及び解読実行手段は、システム制御部１７に対応する）。また、このセキュリティプログラムは、例えばインターネット上の所定のサーバからダウンロードされるようにしてもよいし、フレキシブルディスク（例えば、ＣＤ－ＲＯＭ等）の記録媒体に記録されて当該記録媒体のドライブを介して読み込まれるようにしてもよい。

【図面の簡単な説明】

【００９５】

【図１】本実施形態における車載用オーディオ装置の概要ブロック例を示す図である。

【図２】メモリカード２０への暗号化情報の書き込み時におけるメモリカード制御部１５とメモリカード２０における情報処理及び情報やり取りを示すシーケンス図である。

【図３】メモリカード２０からの暗号化情報の読み出し時におけるメモリカード制御部１５とメモリカード２０における情報処理及び情報やり取りを示すシーケンス図である。

【図４】システム制御部１７におけるメインルーチンの一例を示すフローチャートである。

【図５】図４に示すステップＳ１３の鍵管理処理の詳細を示すフローチャートである。

【図６】（Ａ）は、図５に示すステップＳ２３の暗号化鍵発行処理を示すフローチャートであり、（Ｂ）は、図５に示すステップＳ２５の暗号化鍵回収処理を示すフローチャートであり、（Ｃ）は、図５に示すステップＳ２７のセキュリティＯＮ／ＯＦＦ設定処理を示すフローチャートであり、（Ｄ）は、図５に示すステップＳ２９の暗号化鍵有効／無効設定処理を示すフローチャートである。

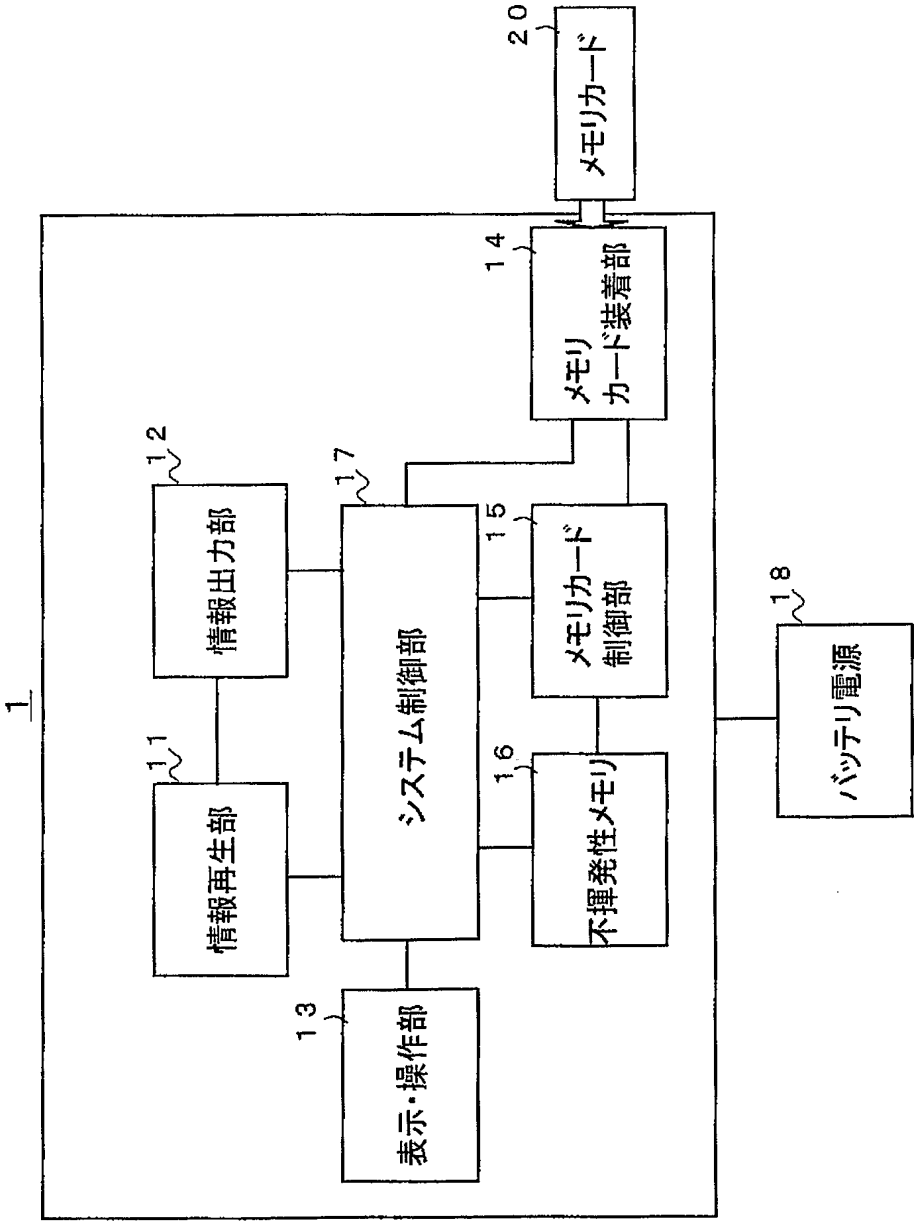
【符号の説明】

【００９６】

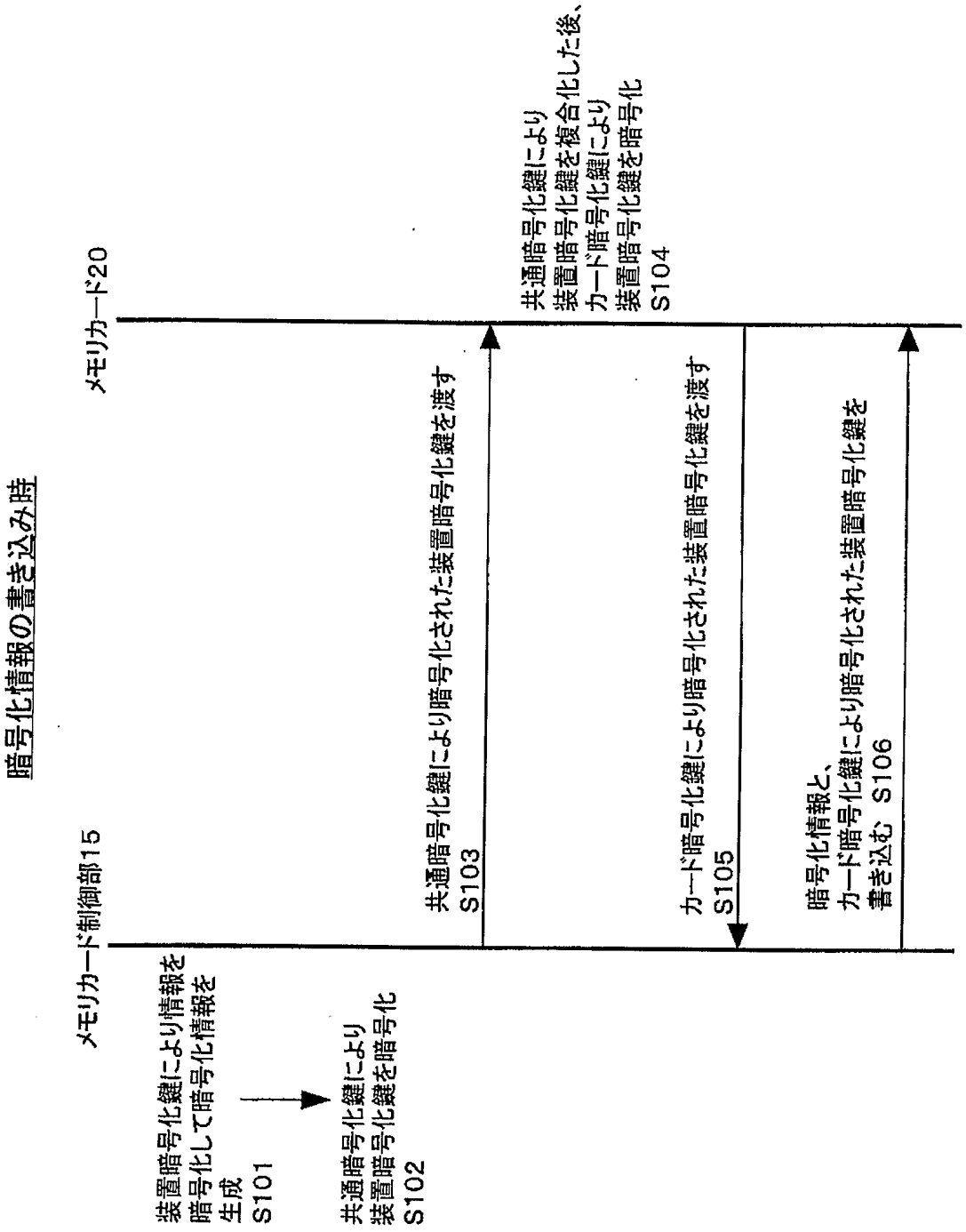
１　車載用オーディオ装置
１１　情報再生部
１２　情報出力部
１３　表示・操作部
１４　メモリカード装着部
１５　メモリカード制御部

１６　不揮発性メモリ
１７　システム制御部
１８　バッテリ電源
２０　メモリカード

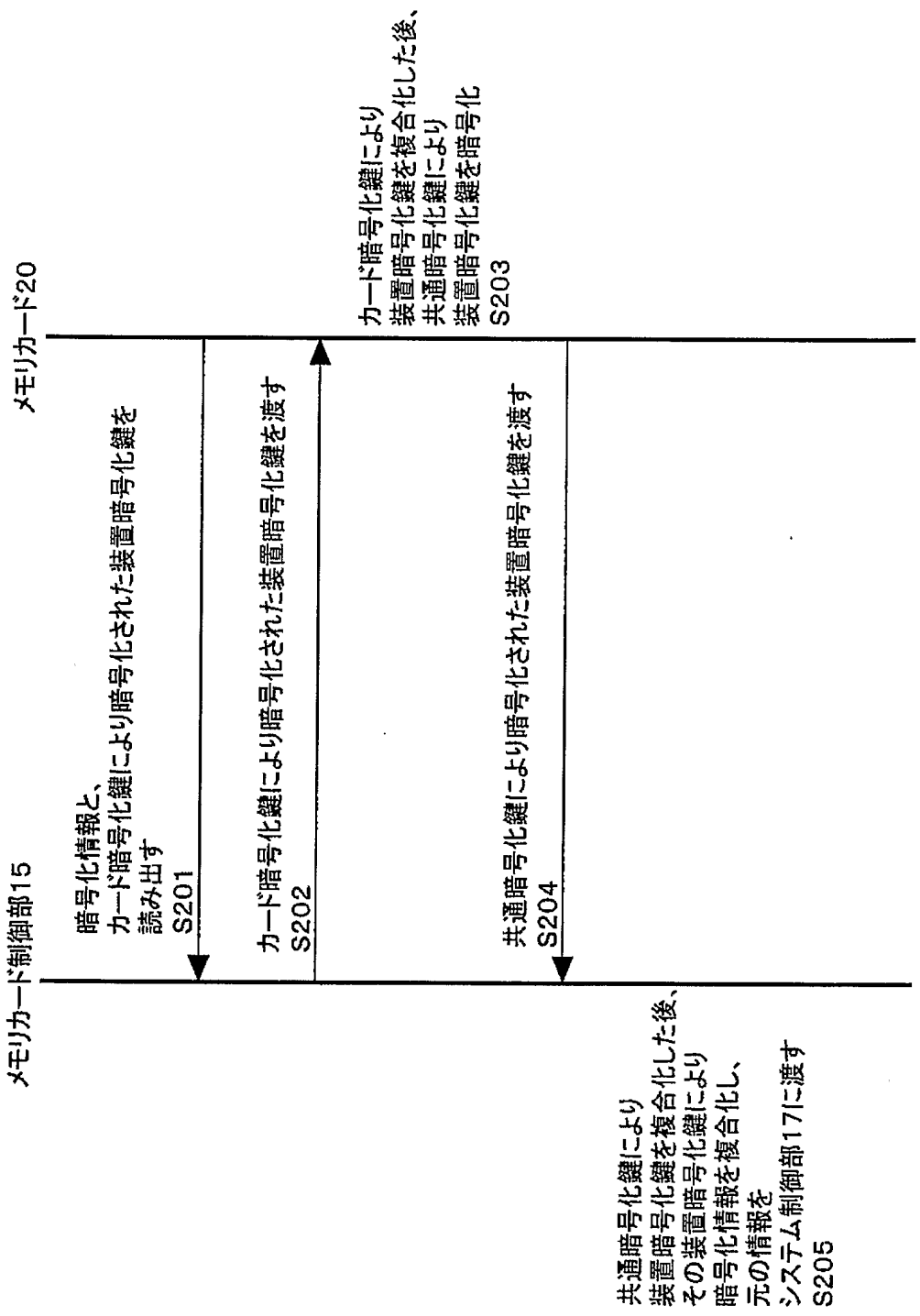
【書類名】図面
【図１】


1
20
メモリカード
14
メモリカード装着部
12
情報出力部
17
システム制御部
15
メモリカード制御部
18
バッテリ電源
11
情報再生部
16
不揮発性メモリ
13
表示・操作部

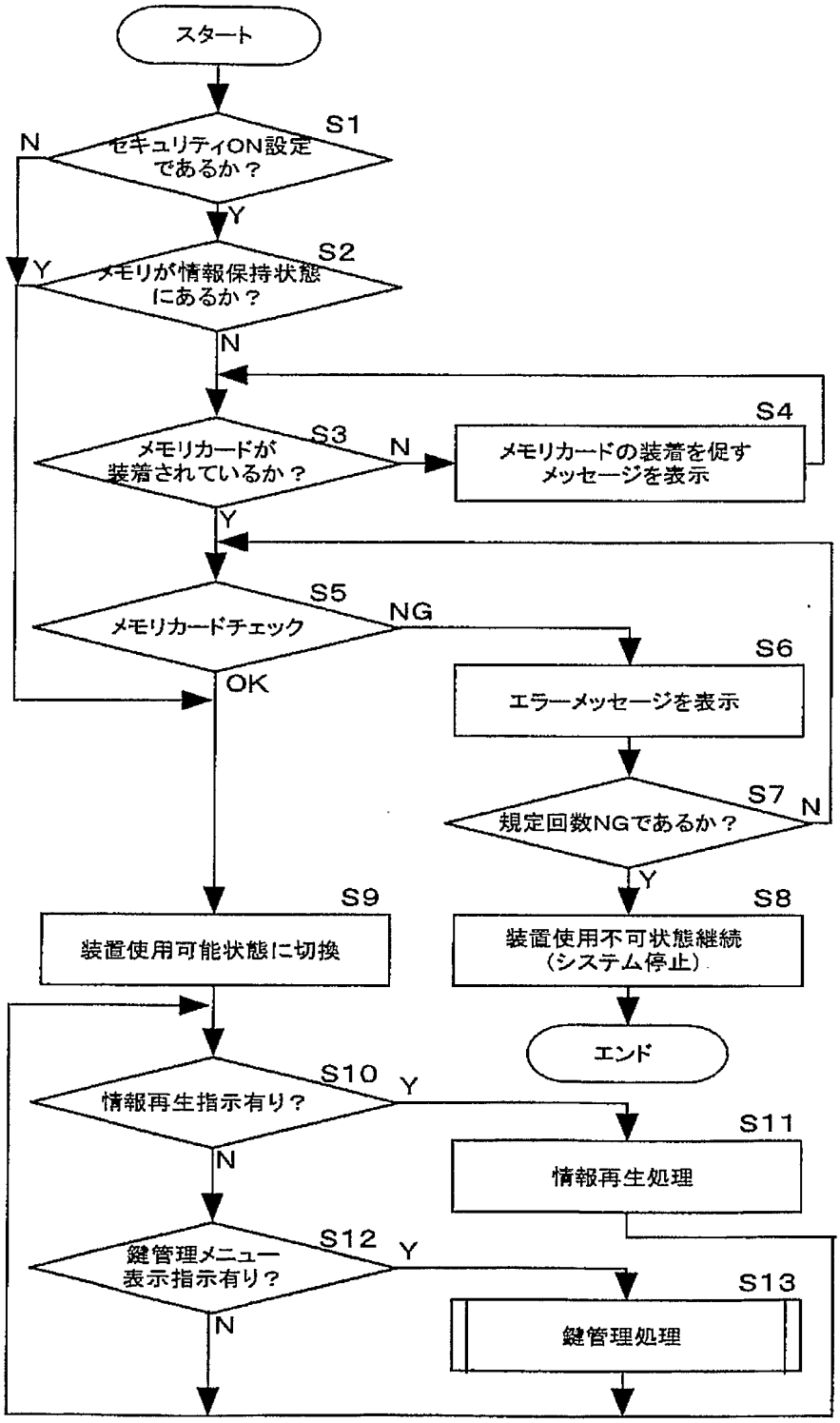
【図２】


暗号化情報の書き込み時
メモリカード制御部15
メモリカード20
装置暗号化鍵により情報を暗号化して暗号化情報を生成
S101
共通暗号化鍵により装置暗号化鍵を暗号化
S102
共通暗号化鍵により暗号化された装置暗号化鍵を渡す
S103
共通暗号化鍵により装置暗号化鍵を複合化した後、カード暗号化鍵により装置暗号化鍵を暗号化
S104
カード暗号化鍵により暗号化された装置暗号化鍵を渡す
S105
暗号化情報と、カード暗号化鍵により暗号化された装置暗号化鍵を書き込む S106

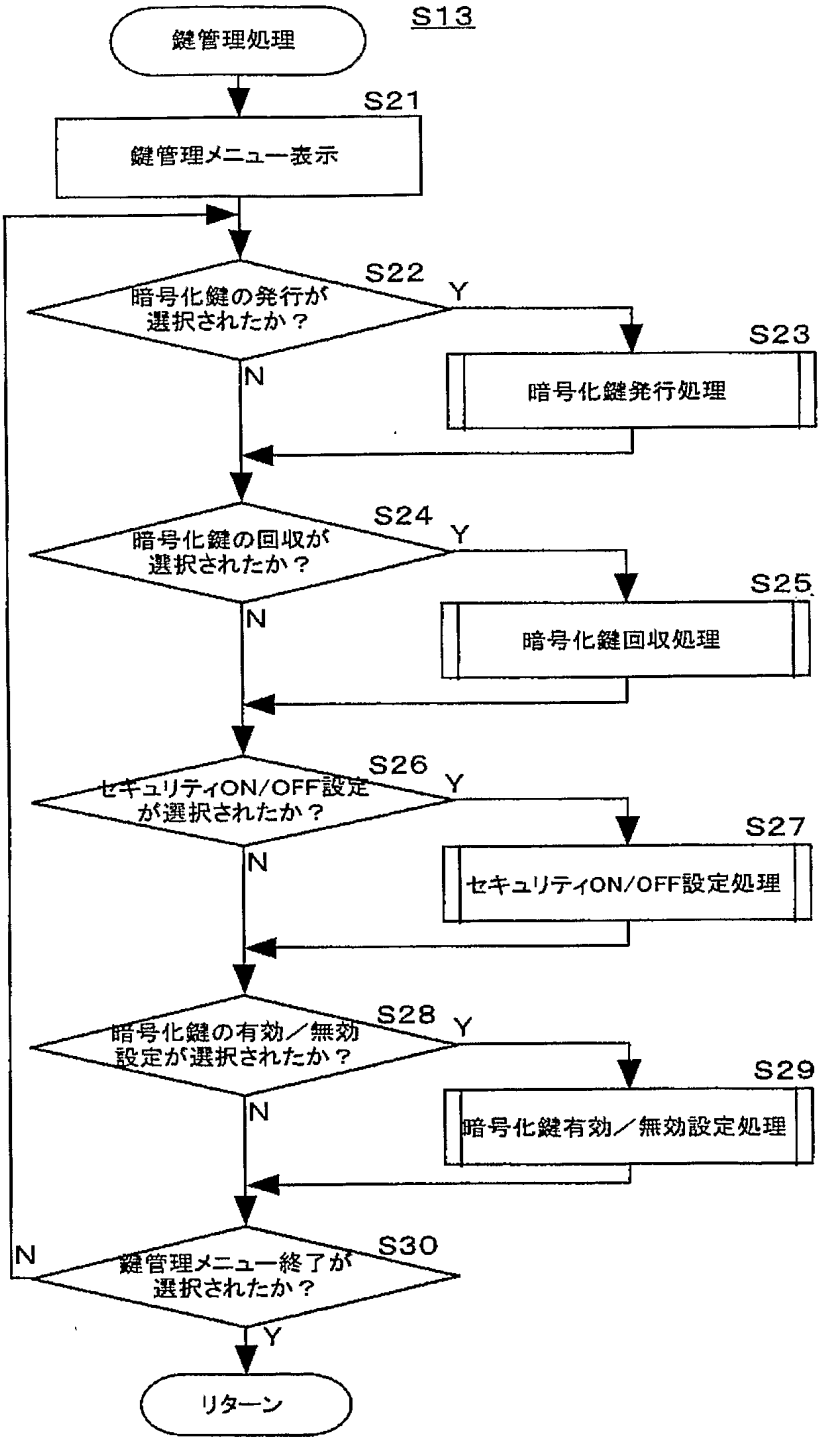
【図３】


暗号化情報の読み出し時
メモリカード制御部15
メモリカード20
暗号化情報と、
カード暗号化鍵により暗号化された装置暗号化鍵を
読み出す
S201
カード暗号化鍵により暗号化された装置暗号化鍵を渡す
S202
カード暗号化鍵により
装置暗号化鍵を複合化した後、
共通暗号化鍵により
装置暗号化鍵を暗号化
S203
共通暗号化鍵により暗号化された装置暗号化鍵を渡す
S204
共通暗号化鍵により
装置暗号化鍵を複合化した後、
その装置暗号化鍵により
暗号化情報を複合化し、
元の情報を
システム制御部17に渡す
S205

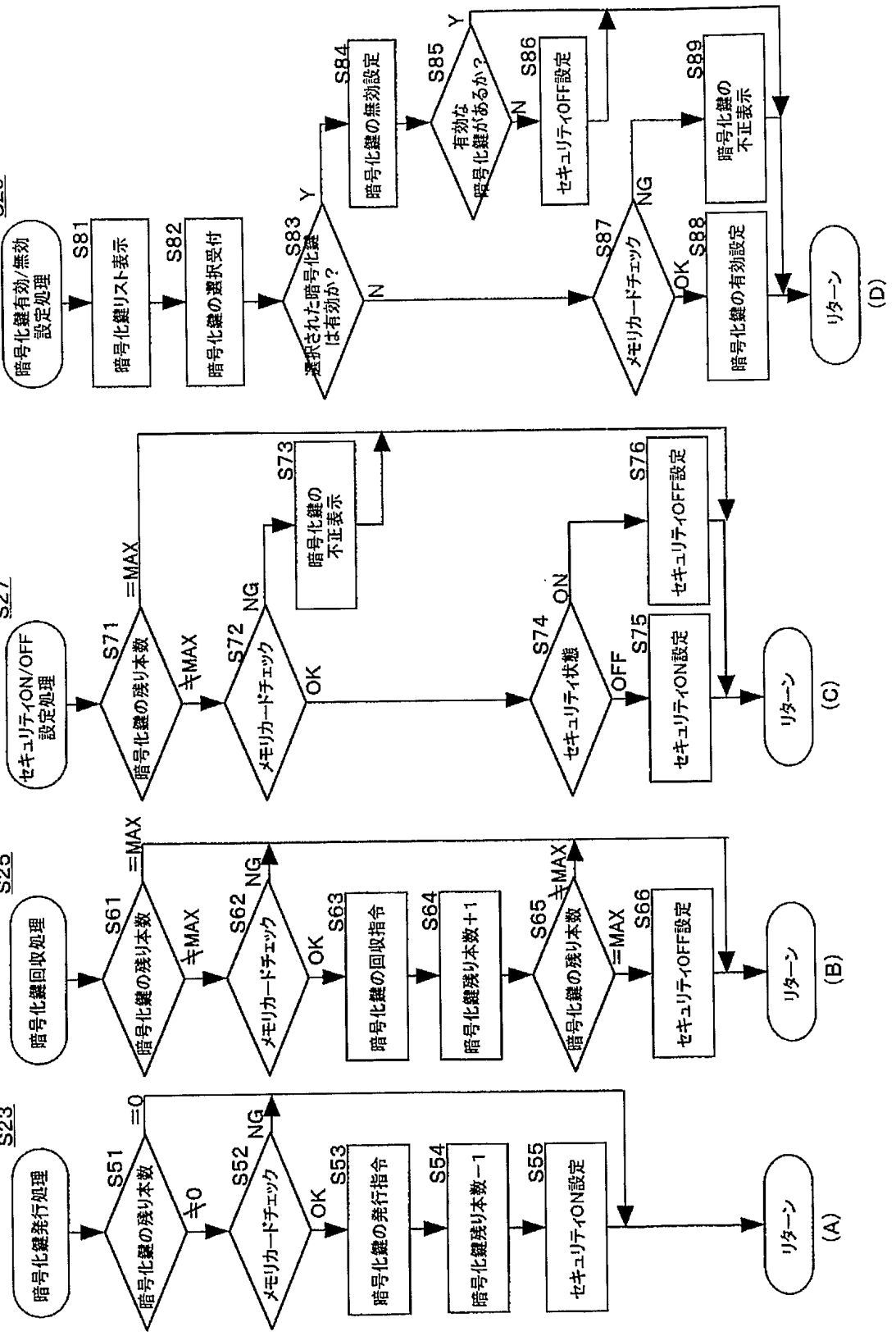
【図４】


スタート
S1
セキュリティON設定であるか？
N
Y
S2
メモリが情報保持状態にあるか？
Y
N
S3
メモリカードが装着されているか？
N
S4
メモリカードの装着を促すメッセージを表示
Y
S5
メモリカードチェック
NG
OK
S6
エラーメッセージを表示
S7
規定回数NGであるか？
N
Y
S8
装置使用不可状態継続（システム停止）
エンド
S9
装置使用可能状態に切換
S10
情報再生指示有り？
Y
N
S11
情報再生処理
S12
鍵管理メニュー表示指示有り？
Y
N
S13
鍵管理処理

【図５】


S13
鍵管理処理
S21
鍵管理メニュー表示
S22
暗号化鍵の発行が選択されたか？
Y
N
S23
暗号化鍵発行処理
S24
暗号化鍵の回収が選択されたか？
Y
N
S25
暗号化鍵回収処理
S26
セキュリティON/OFF設定が選択されたか？
Y
N
S27
セキュリティON/OFF設定処理
S28
暗号化鍵の有効／無効設定が選択されたか？
Y
N
S29
暗号化鍵有効／無効設定処理
S30
鍵管理メニュー終了が選択されたか？
N
Y
リターン

【図６】


S23
暗号化鍵発行処理
S51
暗号化鍵の残り本数
=0
≠0
S52
メモリカードチェック
NG
OK
S53
暗号化鍵の発行指令
S54
暗号化鍵残り本数−1
S55
セキュリティON設定
リターン
(A)
S25
暗号化鍵回収処理
S61
暗号化鍵の残り本数
=MAX
≠MAX
S62
メモリカードチェック
NG
OK
S63
暗号化鍵の回収指令
S64
暗号化鍵残り本数+1
S65
暗号化鍵の残り本数
≠MAX
=MAX
S66
セキュリティOFF設定
リターン
(B)
S27
セキュリティON/OFF
設定処理
S71
暗号化鍵の残り本数
=MAX
≠MAX
S72
メモリカードチェック
NG
OK
S73
暗号化鍵の
不正表示
S74
セキュリティ状態
ON
OFF
S75
セキュリティON設定
S76
セキュリティOFF設定
リターン
(C)
S29
暗号化鍵有効/無効
設定処理
S81
暗号化鍵リスト表示
S82
暗号化鍵の選択受付
S83
選択された暗号化鍵
は有効か？
Y
N
S84
暗号化鍵の無効設定
S85
有効な
暗号化鍵があるか？
Y
N
S86
セキュリティOFF設定
S87
メモリカードチェック
NG
OK
S88
暗号化鍵の有効設定
S89
暗号化鍵の
不正表示
リターン
(D)

【書類名】要約書
【要約】
【課題】　電子機器の盗難を防止又は抑止することが可能な電子機器及びその制御方法、並びにセキュリティプログラム等を提供する。
【解決手段】　携帯型の記録媒体を装着する装着手段と、当該電子機器固有の暗号化鍵を用いて所定の情報を暗号化し、暗号化情報として前記記録媒体に書き込む暗号化情報書込手段と、を備える電子機器であって、前記記録媒体が前記装着手段に装着された場合に、当該記録媒体に記録されている暗号化情報を読み出す暗号化情報読出手段と、前記暗号化鍵を用いて前記暗号化情報の解読を実行する解読実行手段と、前記解読実行手段により前記暗号化情報が解読された場合には、当該電子機器を使用可能状態にさせる制御手段と、を備える。
【選択図】　図４

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２００４－０５８４４４ |
| 受付番号 | ５０４００３４３９７５ |
| 書類名 | 特許願 |
| 担当官 | 第七担当上席　　００９６ |
| 作成日 | 平成１６年　３月　４日 |

＜認定情報・付加情報＞

【提出日】　平成16年 3月 3日

特願２００４－０５８４４４

# 出　願　人　履　歴　情　報

識別番号　　［０００００５０１６］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都目黒区目黒１丁目４番１号
氏　名　　パイオニア株式会社

特願２００４－０５８４４４

出　願　人　履　歴　情　報

識別番号　　［５０２１９６４６３］

１．変更年月日　　２００２年　５月３１日
［変更理由］　　新規登録
住　所　　東京都大田区大森西４丁目１５番５号
氏　名　　株式会社テック・エキスパーツ

特願２００４－０５８４４４

出　願　人　履　歴　情　報

識別番号　［５００４０３９２９］

１．変更年月日　２００２年１０月２３日
［変更理由］　住所変更
住　所　宮城県仙台市青葉区堤町１－１－２　エムズ北仙台５階
氏　名　パイオニアシステムテクノロジー株式会社